

TRAINING | W^3



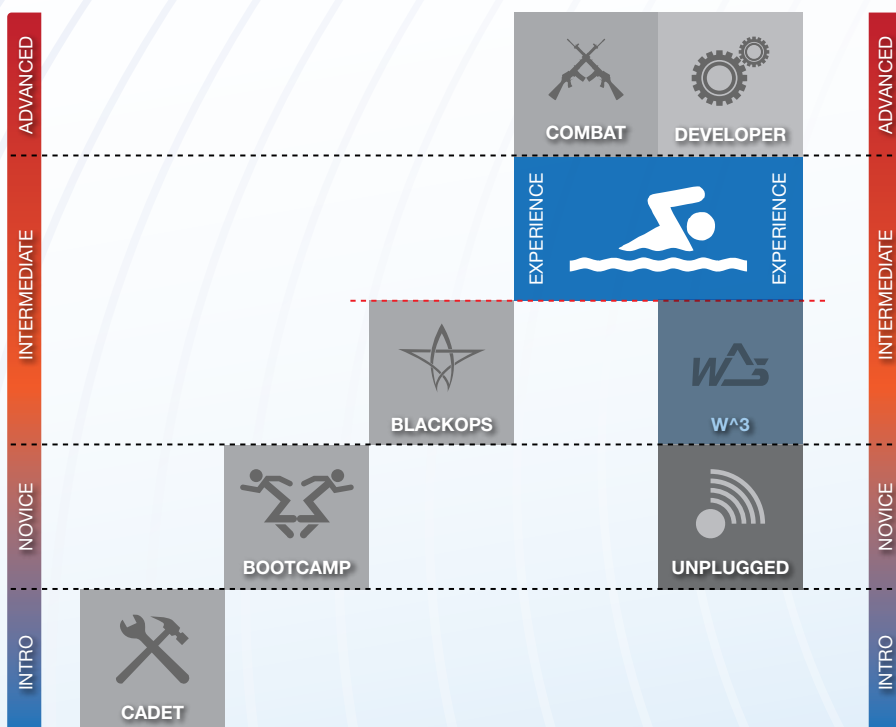
W^3 Edition

“W^3 Edition” is an intermediate web application hacking course for students with some experience in penetration testing.

The course will provide a refresher of HTTP and associated technologies before commencing with more advanced level attacks ranging from assessment techniques of traditional web applications, to newer technologies namely AJAX, rich client media and HTML 5.

As with all courses in the Hacking by Numbers range, the “W^3 Edition” is a hands-on, highly practical course which aims to help students to better understand the trade and not the trick.

Training Overview



SensePost Information Security

Information Security

As trusted advisors we deliver insight, information and systems to enable our customers to make informed decisions about Information Security that support their business performance.

SensePost is an independent and objective organisation specialising in Information Security Consulting, Training, Security Assessment Services and IT Vulnerability Management.

SensePost is about security. Specifically - Information Security. Even more specifically - measuring Information Security.

We’ve made it our mission to develop a set of competencies and services that deliver our customers with insight into the security posture of their information and information systems.

Training Overview

- Cadet Edition
- Cadet Online Edition
- Bootcamp Edition
- BlackOps Edition
- Combat Edition
- Unplugged Edition
- W^3 Edition
- Developer Edition

TRAINING | W[^]3

Content

- HTTP protocol specification
- Automation of HTTP attacks
- Session attacks
- Command execution vulnerabilities
- Traversal vulnerabilities
- File inclusion
- Basic and advanced SQL Injection
- SQL truncation attacks
- Cross-Site Scripting
- Fragmented cross site scripting
- Cross-Site request forgery
- Web2.0 HTTP requests and responses, i.e. JSON etc.
- Advanced XSS with CSRF
- XSS and XmlHttpRequest
- JSON hijacking: Flash and Silverlight
- HTML5
- XML Entity attacks
- XML injection
- LDAP injection
- Post exploitation: UDF uploading, establishing tunnels, pivoting
- Thick application assessment
- Attacking web services

Context

This course is the only one in the Hacking By Numbers series focussing specifically on web-based technologies. This course is an intermediate-level course. It is not mandatory to complete any other SensePost courses before attending this course. However, previous exposure to hacker thinking, tools and techniques is a prerequisite and a basic understanding of web hacking concepts and techniques is assumed.

Prerequisites

SensePost will provide fully configured laptop computers as well as CDs with all the tools and materials used on the course. Students need to ensure they have the necessary level of skill. Some previous hacking experience is required for this course, and a solid technical grounding is an absolute must. It is not mandatory to complete any other SensePost courses before attending this course. However, previous exposure to hacker thinking, tools and techniques is a prerequisite and a basic understanding of web hacking concepts and techniques is assumed. Students without the requisite technical skills are encouraged to consider "Bootcamp Edition". "Bootcamp" and "W[^]3 Edition" can be taken back-to-back.

Who Should Attend

Security Consultants, Government Agencies, Developers and Penetration Testers will all benefit from the valuable insights provided by this course.

"The "W[^]3 Edition" is an intermediate web application hacking course for people with some experience in penetration testing."

More Training At SensePost



CADET

Cadet Edition

is an introductory course for technical students with no previous experience in the world of hacking. The course will present the student background information, technical skills and basic concepts required to get the student going.



BOOTCAMP

Bootcamp Edition

is the core of the HBN series. A highly practical course that teaches method-based hacker thinking, skills and techniques. This course continues to receive support and acclaim from all over the world.



BLACKOPS

BlackOps Edition

is a course to sharpen the student's skills in real scenarios before being shipped off to battle. "BlackOps" covers tools and techniques to brush up skills on data exfiltration, privilege escalation, pivoting, client-side attacks and exploit writing.



COMBAT

Combat Edition

is a unique concept - a series of carefully crafted Capture-The-Flag "missions", each designed to teach a specific hacking skill or concept. This course is all hack, no talk. "Combat" has been described as "Zen" for hackers.



UNPLUGGED

Unplugged Edition

is the ultimate wi-fi hacking course. With a strong focus on obtaining results in offensive scenarios for wi-fi hacking. Presents students with the background knowledge, methodologies, tools and thinking skills required.



W[^]3

W[^]3 Edition

is an intermediate web application hacking course for students with some experience in penetration testing. "W[^]3" is a hands-on, highly practical course which aims to enable students to understand the trade and not the trick of breaking webapps.



DEVELOPER

Developer Edition

introduces a wide array of common (and not so common) web application security vulnerabilities. Students are given hands-on lab exercises allowing them to attack vulnerable applications and to fully explore the impact of potentially vulnerable code.